PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-187306
(43)Date of publication of application : 02.07.2004

(51)Int.Cl. H04L 9/16
H04L 12/56
H04N 7/08
H04N 7/081
H04N 7/16

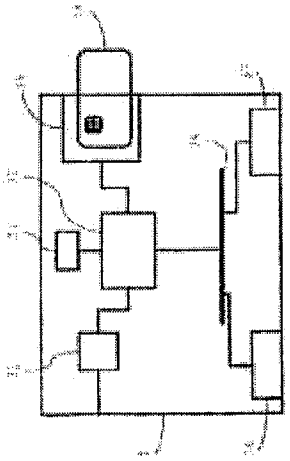
(21)Application number : 2003-406448
(22)Date of filing : 04.12.2003

(71)Applicant : IRDETO ACCESS BV
(72)Inventor : RANJAN KARTHIK

(30)Priority
Priority number : 2002 02080137 Priority date : 04.12.2002 Priority country : EP

(54) TERMINAL FOR RETRANSMITTING DIGITAL DATA, TERMINAL WITH METHOD THEREOF, AND DATA DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a terminal for receiving and retransmitting information.
SOLUTION: The present invention provides a first network adapter (31, 36) for encoding information to receive a first data stream encrypted by a key scheme from a first transmitter (25, 26, 27) via a first network within a first format, a device for receiving an entitlement message to enable an authorized receiver to decrypt the encrypted data stream, and at least another network adapter (37) for connection to a second network (2).



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-187306
(P2004-187306A)
(43)公開日　平成16年7月2日(2004.7.2)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/16	H04L	9/00	643	5C063
H04L	12/56	H04L	12/56	Z	5C064
H04N	7/08	H04N	7/16	Z	5J104
H04N	7/081	H04N	7/08	Z	5K030
H04N	7/16				

審査請求 未請求　請求項の数 15　OL　（全 15 頁）

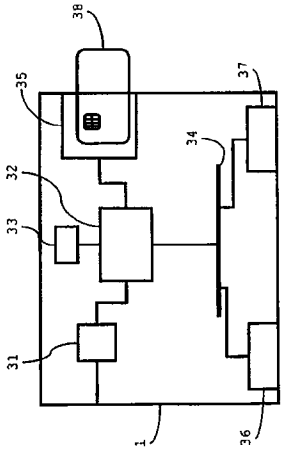
(21)出願番号　特願2003-406448(P2003-406448)
(22)出願日　平成15年12月4日(2003.12.4)
(31)優先権主張番号　02080137.9
(32)優先日　平成14年12月4日(2002.12.4)
(33)優先権主張国　欧州特許庁(EP)

(71)出願人　500232617
イルデト・アクセス・ベー・フェー
オランダ・ＮＬ－２１３２・ＨＤ・ハーフドドープ・ジュピターストラート・４２
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108578
弁理士　高橋　詔男
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100101465
弁理士　青山　正和
(74)代理人　100094400
弁理士　鈴木　三義

最終頁に続く

(54)【発明の名称】デジタルデータを再送信する端末及び方法を具備する端末及びデータ配信システム

(57)【要約】
【課題】　情報を受信及び再送信するための端末を提供する。
【解決手段】　情報が符号化され、第１フォーマット内の第１ネットワークを介して第１送信器(25,26,27)からのキースキームによって暗号化された第１データストリームを受信するための第１ネットワークアダプタ(31,36)と、認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを受信するための装置と、第２ネットワーク(2)へ接続するための少なくとも１つの別のネットワークアダプタ(37)とを備える。
【選択図】　図３



【特許請求の範囲】
【請求項１】
情報を受信及び再送信するための端末であって、
前記端末は、
前記情報が符号化され、第１フォーマット内の第１ネットワークを介して第１送信器(25,26,27)からのキースキームによって暗号化された第１データストリームを受信するための第１ネットワークアダプタ(31,36)と、
認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを受信するための装置と、
第２ネットワーク(2)へ接続するための少なくとも１つの別のネットワークアダプタ(37)とを備え、
前記端末は、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内の前記情報の少なくとも一部を、前記第２ネットワーク(2)に接続された少なくとも１つの第２端末(3,5,6)に前記第２ネットワークを介して再送信するように構成されるとともに、
前記端末は、同じキースキームによって暗号化された前記第２データストリームを送信するとともに、認可された受信器が前記第２データストリームを解読することができる受信エンタイトルメントメッセージを前記第２端末(3,5,6)に転送するように構成されることを特徴とする端末。
【請求項２】
前記端末は、受信された前記第１データストリームを復号化するとともに、前記キースキームによって前記第２データストリームを暗号化するために実施されることを特徴とする請求項１に記載の端末。
【請求項３】
前記端末は、複数の基本データストリームを具備する解読データストリームを逆多重化するとともに、前記基本データストリームのサブセット内で符号化された情報を再送信するように構成されることを特徴とする請求項２に記載の端末。
【請求項４】
前記端末は、前記第２端末からの選択コマンドを受信するとともに、前記選択コマンドによって前記一部に具備された前記基本データストリームを選択するように構成されることを特徴とする請求項３に記載の端末。
【請求項５】
前記端末は、第１データパケットフォーマット内の暗号化された前記第１データストリームを受信するとともに、第２データパケットフォーマット内の少なくとも１つの第２ストリームに送信するように構成されることを特徴とする請求項１ないし請求項４のうちいずれか１に記載の端末。
【請求項６】
前記端末は、前記第１データパケットフォーマット内の受信された暗号化データパケット(14,39,42)のペイロード(13,17)を解読し、解読された前記ペイロードからクリアデータを形成し、前記第２データパケットフォーマットに一致するクリアデータをその次に再パケット化するように構成されることを特徴とする請求項１ないし請求項５のうちいずれか１に記載の端末。
【請求項７】
前記端末は、多数の暗号化された基本データストリームを具備する暗号化データストリームを逆多重化するとともに、前記基本データストリームのサブセットを再送信するようにに構成されることを特徴とする請求項２、請求項５、請求項６に記載の端末。
【請求項８】
前記端末は、送信された前記第２データストリーム内の１つまたはそれ以上の第２端末(3,5,6)を識別する１つまたはそれ以上のアドレス(44)を含むように構成されることを特徴とする請求項１ないし請求項７のうちいずれか１に記載の端末。

【請求項９】
前記端末は、第１フォーマット内の符号化された情報を具備する第１データストリームを受信し、第２フォーマット内に前記情報を符号化し、少なくとも１つの前記第２データストリーム内に再符号化された前記情報を具備するデータを含むように構成されることを特徴とする請求項１ないし請求項８のうちいずれか１に記載の端末。
【請求項１０】
前記端末は、第１スキームに基づいて圧縮されたデータを具備する第１データストリームを受信し、前記データを逆圧縮し、第２スキームに基づいて前記データを再圧縮し、少なくとも１つの前記第２データストリーム内の再圧縮された前記データを含むために実施されることを特徴とする請求項９に記載の端末。
【請求項１１】
前記端末は、少なくとも１つの前記第２端末(3,5,6)に少なくとも１つの前記第２データストリームの送信を認可するメッセージを受信し、権限が受信されるそれらの第２端末(3,5,6)にそれら第２データストリームのみを送信するように構成されることを特徴とする請求項１ないし請求項１０のうちいずれか１に記載の端末。
【請求項１２】
認可された受信器が前記キースキームによって暗号化された暗号化データストリームを解読することができる複数の異なるエンタイトルメントメッセージを受信するための装置を備え、前記エンタイトルメントメッセージそれぞれは、少なくとも１つの端末の規格を備え、
前記端末は、前記第２端末(3,5,6)が一致する規格を具備するそれらのエンタイトルメントメッセージのみ、前記第２端末(3,5,6)に転送するように構成されることを特徴とする請求項１ないし請求項１１のうちいずれか１に記載の端末。
【請求項１３】
第１ネットワークと、
前記第１ネットワークに接続されるとともに、第１フォーマット内の前記第１ネットワークを介したキースキームによって暗号化された暗号化第１データストリーム内で符号化された情報を送信するように構成される第１データ送信器(25,26,27)と、
認可された受信器が前記暗号化データストリームを復号化できるようなエンタイトルメントメッセージを送信するように構成されるエンタイトルメントメッセージ送信器(25,26,27)と、
第２ネットワーク(2)と、
前記第２ネットワーク(2)に接続された１つまたはそれ以上の第２端末(3,5,6)と、
前記第１ネットワークおよび前記第２ネットワーク(2)に接続され、前記第１ネットワークを介して前記第１データ送信器(25,26,27)から前記暗号化データストリームを受信するとともに、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内で符号化された前記情報の少なくとも一部を、前記第２ネットワーク(2)に接続された１つまたはそれ以上の第２端末(3,5,6)に再送信するように構成される第１端末（1）とを備え、
前記第１端末(1)は、同じキースキームによって暗号化された前記第２データストリームを送信するとともに、認可された受信器が前記第２端末(3,5,6)への前記第２データストリームを解読できる受信エンタイトルメントメッセージを転送するように構成されることを特徴とするデジタルデータ配信システム。
【請求項１４】
第１フォーマット内の第１ネットワークを介した第１送信器(25,26,27)からのキースキームによって暗号化された暗号化第１データストリーム内で符号化された情報を受信する段階と、
認可された受信器が前記暗号化データストリームを解読できるエンタイトルメントメッセージを受信する段階と、
前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データスト

リーム内で符号化された前記情報の少なくとも一部を、第２ネットワーク(2)を介して少なくとも１つの第２端末(3,5,6)に再送信する段階とを備え、

前記第２データストリームは、前記同じキースキームによって暗号化され、送信され、そして、認可された受信器が前記第２データストリームを解読できる受信エンタイトルメントメッセージが前記第２端末(3,5,6)に転送されることを特徴とするデジタルデータを受信及び再転送する方法。

【請求項１５】

デジタルデータを受信及び再送信するための端末(1)にローディングするのに適したコンピュータプログラムであって、

プロセッサ(32)と、

メモリ(33)と、

第１フォーマット内の第１ネットワークを介して第１送信器(25,26,27)からデータストリームを受信するための第１ネットワークアダプタ(31,36)と、

認可された受信器が暗号化データストリームを解読できるエンタイトルメントメッセージを受信するための装置と、

第２ネットワーク(2)に接続するための少なくとも１つの別のネットワークアダプタ(37)とを備え、

この方法でプログラムされた端末(1)は、請求項１ないし１２のいずれか１に記載の端末の前記機能が提供されることを特徴とするデジタルデータを受信及び再送信するための端末(1)にローディングするのに適したコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク境界(network boundaries)での転送制御(transcontrol)の分野に関する。

【０００２】

特に、本発明は、情報を受信及び再送信(re-transmitting)するための端末に関し、前記端末は、前記情報が符号化され、第１フォーマット内の第１ネットワークを介して第１送信器からのキースキームによって暗号化された第１(primary)データストリームを受信するための第１ネットワークアダプタと、認可された受信器(authorized receiver)が前記暗号化データストリームを復号化できるようにするエンタイトルメントメッセージ(entitlement messages)を受信するための装置(arrangement)と、第２ネットワークへ接続するための少なくとも１つの別の(further)ネットワークアダプタとを具備する。前記端末は、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内の前記情報の少なくとも一部を、前記第２ネットワークに接続された少なくとも１つの第２端末に前記第２ネットワークを介して再送信するように構成されている。

【０００３】

さらに本発明は、デジタルデータ配信システムに関し、前記デジタルデータ配信システムは、第１ネットワークと、前記第１ネットワークに接続されるとともに、第１フォーマット内の前記第１ネットワークを介したキースキームによって暗号化された暗号化第１データストリーム内で符号化された情報を送信するために構成された(arranged to)第１データ送信器と、認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを送信するために実施されるエンタイトルメントメッセージ送信器と、第２ネットワークと、前記第２ネットワークに接続された１つまたはそれ以上の第２端末と、前記第１ネットワークおよび前記第２ネットワークに接続され、前記第１ネットワークを介して前記第１データ送信器から前記暗号化データストリームを受信するとともに、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内で符号化された前記情報の少なくとも一部を、前記第２ネットワークに接続された１つまたはそれ以上の第２端末に再送信するように構成された第１端末とを

具備する。

【０００４】

また、本発明は、デジタルデータを受信及び再送信する方法に関し、前記方法は、第１フォーマット内の第１ネットワークを介した第１送信器からのキースキームによって暗号化された暗号化第１データストリームで符号化された情報を受信する段階と、認可された受信器が前記暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信する段階と、前記第１フォーマットと異なる第２フォーマット内で少なくとも１つの第２データストリーム内に符号化された前記情報の少なくとも一部を、第２ネットワークを介して少なくとも１つの第２端末に再送信する段階とを備える。

【０００５】

さらに、本発明は、デジタルデータを受信及び再送信するための端末にローディングするのに適したコンピュータプログラムに関し、前記端末は、プロセッサと、メモリと、第１フォーマット内の第１ネットワークを介して第１送信器からデータストリームを受信するための第１ネットワークアダプタと、認可された受信器が暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信するための装置と、第２ネットワークに接続するための少なくとも１つの別のネットワークアダプタとを備える。

【背景技術】

【０００６】

そのような端末、システム及び方法の例は、例えば、特許文献１によって公知である。この公報には、ビデオケーブル及びIEEE 1394ケーブルを介してテレビジョン受信器に接続されるセットトップボックスが開示されている。フロントエンド回路(front end circuit)は、ユーザの局選択に対応する放送信号を、アンテナからのDSS（ダイレクト衛星システム(Direct Satellite System)）入力から抽出するとともに、デスクランブル回路(descramble circuit)にそれを出力する。充電回路は、スクランブル解除のための復号化キーを前記デスクランブル回路に供給する。マルチプレクスエディティング回路（多重化編集回路(multiplex editing circuit)）は、タイムスタンプ及び（MPEG符号化された）HD放送信号のパケット長さを、前記デスクランブル回路からIEEE 1394で定義されたトランスポートストリームに再配置(rearranges)するとともに、次いで、暗号化回路にそれを出力する。関係している(concerned)前記放送信号がペイパービュー(pay per view)である場合、前記暗号化回路は、前記マルチプレクスエディティング回路からの前記トランスポートストリームを暗号化する。コントローラは、磁気ディスク、光ディスク、光磁気ディスクまたは半導体メモリに記憶された制御プログラムを読み出すためにドライブを制御するとともに、読み出された前記制御プログラム及びユーザからのコマンド入力などに基づいて、前記セットトップボックスの各回路を制御する。前記充電回路は、前記暗号化回路に接続されていない。

【０００７】

前記公知端末が用いられるとき、前記第１送信器からのエンティティ(entity)送信データは、前記データが前記第１端末で解読されるとすぐに制御を解除する。次に、前記復号化データが再暗号化されたとしても、このエンティティは、もはや前記データへのアクセスを制御しない。前記第２ネットワークを介した前記データの受信及び再送信のために用いられる前記第１端末のオペレータは、前記データストリームを再暗号化するために用いられたキーをそれらに送信することによって、前記再暗号化データストリームの解読が可能な第２受信器を決定できる。

【０００８】

【特許文献１】ヨーロッパ特許公開公報1089470

【発明の開示】

【発明が解決しようとする課題】

【０００９】

本発明は、デジタルデータの第１提供者が第２ネットワークを介して前記データの別の配信の制御を実行し続けることができるような、上述のタイプの端末、システム及び方法

を提供する。

【課題を解決するための手段】

【００１０】

本発明は、情報を受信及び再送信するための端末を提供することによってこれを達成する。前記端末は、第１フォーマットで第１ネットワークを介して第１送信器からのキースキームにより暗号化された第１データストリームを受信するための第１ネットワークアダプタと、認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを受信するための装置と、第２ネットワークへ接続するための少なくとも１つの別のネットワークアダプタとを備える。前記端末は、前記第１フォーマットと異なる第２フォーマットで少なくとも１つの第２データストリーム内の前記情報の少なくとも一部を、前記第２ネットワークに接続された少なくとも１つの第２端末に前記第２ネットワークを介して再送信するように構成される。前記端末は、同じキースキームによって暗号化された前記第２データストリームを送信するとともに、認可された受信器が前記第２データストリームを解読することができる受信されたエンタイトルメントメッセージを前記第２端末に転送するように構成される。

【００１１】

転送されたエンタイトルメントメッセージ（すなわち、前記情報を前記端末に供給するソースによって生成されるエンタイトルメッセージ）は、前記第２受信器が前記再送信されたデータストリームを解読することができるように用いられるので、前記第１データ提供者は、前記データの別の配信の制御を実行し続ける。

【００１２】

好適には、前記端末は、受信された前記第１データストリームを解読するとともに、前記キースキームによって前記第２データストリームを暗号化するように構成される。

【００１３】

従って、前記端末は、受信された前記データストリーム、例えば、多重化されたストリーム内の特定の基本ストリーム内に具備された前記データにアクセスしてもよい。このように、それ（前記端末）は、情報、例えば、受信された前記データストリームの各部をどちらに転送するか決定するために利用される基本(elementary)ストリームを識別する識別子のテーブルにアクセスできる。

【００１４】

本発明の他の形態によると、デジタルデータ配信システムが提供される。前記デジタルデータ配信システムは、第１ネットワークと、前記第１データネットワークに接続されるとともに、第１フォーマット内の前記第１ネットワークを介したキースキームによって暗号化された暗号化第１データストリーム内で符号化された情報を送信するために実施される第１データ送信器と、認可された受信器が前記暗号化データストリームを解読できるようにするエンタイトルメントメッセージを送信するように構成されるエンタイトルメントメッセージ送信器と、第２ネットワークと、前記第２ネットワークに接続された１つまたはそれ以上の第２端末と、前記第１ネットワークおよび前記第２ネットワークに接続され、前記第１ネットワークを介して前記第１データ送信器から前記暗号化データストリームを受信するとともに、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内で符号化された前記情報の少なくとも一部を、前記第２ネットワークに接続された１つまたはそれ以上の第２端末に再送信するために実施される第１端末とを備え、前記第１端末は、同じキースキームによって暗号化された前記第２データストリームを送信するとともに、認可された受信器が前記第２端末への前記第２データストリームを解読できるようにする受信されたエンタイトルメントメッセージを転送するように構成される。

【００１５】

前記システムは、前記第１データ送信器を用いるエンティティが、前記第２端末に再送信される前記データを制御し続けることができるようにする。

【００１６】

本発明の別の形態によると、デジタルデータを受信及び再転送する方法が提供される。デジタルデータを受信及び再転送する方法は、第１フォーマット内の第１ネットワークを介した第１送信器からのキースキームによって暗号化された暗号化第１データストリーム内で符号化された情報を受信する段階と、認可された受信器が前記暗号化データストリームを解読できるようなエンタイトルメントメッセージを受信する段階と、前記第１フォーマットと異なる第２フォーマット内の少なくとも１つの第２データストリーム内で符号化された前記情報の少なくとも一部を、第２ネットワークを介して少なくとも１つの第２端末に再送信する段階とを備え、前記第２データストリームは、前記同じキースキームによって送信され、暗号化され、そして、認可された受信器が前記第２データストリームを解読できるような受信されたエンタイトルメントメッセージが前記第２端末に転送される。

【００１７】

これは、本発明による前記端末によって実行される方法である。

【００１８】

本発明の最後の形態によると、デジタルデータを受信及び再送信するための端末にローディングするのに適したコンピュータプログラムが提供され、前記端末は、プロセッサと、メモリと、第１フォーマット内の第１ネットワークを介して第１送信器からデータストリームを受信するための第１ネットワークアダプタと、認可された受信器が暗号化データストリームを復号化できるようなエンタイトルメントメッセージを受信するための装置と、第２ネットワークに接続するための少なくとも１つの別のネットワークアダプタとを備える。故に、この方法でプログラムされた端末は、本発明による端末の前記機能が提供される。

【００１９】

従って、前記正当なハードウエアを伴う端末は、エンドユーザに至るまで前記コンテンツの配信を制御するさらなる確実性を、コンテンツ提供者に提供する本発明による端末としての機能に容易に適合される。

【発明を実施するための最良の形態】

【００２０】

ここで、本発明は、添付の図面を参照してさらに詳細に説明される。

【００２１】

図１を参照すると、本発明は、２つのネットワーク、すなわち、この例では、配信ネットワークとホームネットワーク2との間のゲートウェイとして用いられる第１受信器1を提供する。前記第１受信器1は、第１フォーマットでデータを受信するとともに、第２フォーマットでそれを再送信する。本発明は、シングルタイプのデータに限られるものではないが、この説明においては、MPEG-2トランスポートストリームパケットが、前記ホームネットワーク2を介して複数の第２受信器にそれら（データ）を再送信する前記第１受信器1に配信される例に焦点をあてる。図１に示されるように、第２受信器の例は、アナログテレビジョンセット4に接続されるセットトップボックス3と、デジタルテレビジョンセット5と、パーソナルコンピュータ6とである。パーソナルコンピュータ6は、ネットワークカードと、メディアプレイヤと、スマートカードリーダ7とを備える。また、本発明は、放送環境に用いられるとは限られない。すなわち、前記第１受信器1は、また、ポイントツーポイント接続を介してソースから前記デジタルデータを受信してもよい。

【００２２】

前記MPEG-2スタンダードISO/IEC 13818はある程度詳しく、データ符号化方法及び転送方法について記載している。この記載は、本発明に関する他の形態を本質的に詳述する。標準についてさらに詳細に知るためには、参照する必要があるかも知れない。

【００２３】

図１において、放送ソース8は、基本ストリーム9をシングルプログラムMPEG-2トランスポートストリーム10に符号化する。基本ストリームは、例えば、ビデオまたはオーディオのようなプログラムの、単にデジタルコード化されるとともに、MPEG-圧縮されたコンポーネントである。プログラムに属するいくつかの基本ストリームからのデータは、プログ

ラム基本ストリーム(PES)パケット11に組み込まれる(carried in)（図２参照）。プログラムは、アナログ放送内のチャンネルに対応している。前記PESパケット11は、PESパケットヘッダ12及びPESパケットペイロード13を具備する。前記基本ストリームからのデータは、前記PESパケットペイロード13がどの基本ストリームに属するかを示す前記PESパケットヘッダ12とともにを伴った前記PESパケット11内に多重化される。

【００２４】

前記PESパケット11は、MPEG-トランスポートストリーム(TS)パケット14（図２）によって運ばれる。MPEG-マルチプレクサ15（図１）は、複数のトランスポートストリームを１つのマルチプログラムトランスポートストリームに多重化する。故に、複数のプログラムが１つのストリームで運ばれる。各TSパケット14（図２）は、TSパケットヘッダ16及びTSパケットペイロード17を具備している。さらに、適応フィールド(adaptation field)18は、それら（各TSパケット14）が運ぶ前記PESパケット11の長さに関係なく、全TSパケット14が同じ長さになるようにする。前記TSパケットヘッダ16は、数ある中で、パケット識別子(PID)19を具備している。前記パケット識別子19は、シングルまたはマルチプログラムトランスポートストリーム内のプログラムの基本ストリームを関連付けるために用いられる独自の整数値である。

【００２５】

PID値０を伴う前記TSパケット14内のプログラムアソシエーションテーブル(PAT)は、前記トランスポートストリーム内で利用可能な全プログラムのリストを具備する。前記PAT内の各プログラムは、前記プログラム及びそれ（プログラム）が具備される前記基本ストリームについての詳細を明らかにするプログラムマップテーブル(PMT)に関連付けられる。

【００２６】

再び図１を参照すると、ネットワークアダプタ20は、総括局(regional center)22への前記TSパケット14を、第１ネットワーク21を介した送信に適したフォーマットに変換する。前記総括局は、ネットワークアダプタ23を介して前記トランスポートストリームを受信する。ビットストリームスプライサ/マルチプレクサ24は、サービス情報(SI)、電子プログラムガイド(EPG)及び文字放送を含む可能性のある他のトランスポートストリームをスプライスする（つなぎ合わせる）ために用いられる。前記ビットストリームスプライサ/マルチプレクサ24は、値の不一致を避けるために、前記PID値及び前記PMTと前記PATを更新する。次いで、前記結果として伴うMPEGトランスポートストリームは、前記第１ネットワーク21を介して、適切なネットワークアダプタ28及び29を用いる衛星送信器25、地上送信器26またはケーブル送信器27にリンクアップされる(linked up)。

【００２７】

衛星、地上またはケーブルネットワークは、受信者の家庭に前記データを配信するために配信ネットワークを形成する。他の適切なネットワークのタイプは、ADSL（非対称デジタル加入者線）、イーサネット(登録商標) 接続などのホーム接続のためにファイバーを使用しているものである。本発明のコンテキスト(context)において、前記配信ネットワークは前記第１ネットワークとして参照される。

【００２８】

前記放送ソース8または前記総括局22のいずれか一方、または前記放送ソース8と前記総括局22の両方は、リンクアップされる前記データストリームのコンテンツへの認可されていないアクセスを防ぐために条件付きアクセスシステム(conditional access system)を用いてもよい。この目的のために、前記PESパケットペイロード13または前記TSパケットペイロード17のいずれか一方がスクランブルされる。ここで留意すべきことは、実際には各々が１つの基本ストリームを運ぶ多重化トランスポートストリームにおいて、複数のトランスポートストリームを具備し、前記トランスポートストリームのサブセットのみがスクランブルされてもよいことである。前記PESパケットヘッダ12またはTSパケットヘッダ16内のフィールドは、それ特有のパケットの前記ペイロードが暗号化されたか否かを示している。説明を複雑にするのを避けるために、スクランブリングは、前記トランスポート

ストリームレベルで実行されるものと仮定する。好適には、DESのような対称暗号化アルゴリズムが前記TSパケットペイロード17をスクランブルするために用いられる。

【００２９】

PID値に関係なく、同一のキー及び/またはアルゴリズムを使って前記TSパケットペイロード17全てをスクランブルすること、または、各基本ストリームまたは１つのプログラムに属する基本ストリームの各セットに対して、異なるキー及び/またはアルゴリズムを用いることが可能であることが知られている。前記総括局22がCAシステムマネージャであると仮定すると、それは、エンタイトルメント制御メッセージを含む１つまたはそれ以上のトランスポートストリームをスプライスする。さらに、CAシステムで用いられるタイプ及び前記エンタイトルメントメッセージの前記PIDを詳細したCA記述子をそれに追加することによって、スクランブルされた前記プログラムに対する前記PMTを修正する。前記エンタイトルメント制御メッセージは、制御語、スクランブリング及びデスクランブリングのために用いられるキーを具備している。エンタイトルメント制御メッセージ(ECMs)は、異なったキーによってそれら自身を暗号化する。別のデータストリームは、認可された加入者または加入者のグループが、前記制御語を取り出せる前記ECMsを解読できるようなエンタイトルメントマネージメントメッセージ(entitlement management messages)を具備する。

【００３０】

図１に戻ると、第１受信器1は、それ（第１受信器）が接続される衛星放送受信アンテナ30によって前記MPEG-2トランスポートストリームを受信する。前記トランスポートストリームは、衛星配信ネットワークを介した送信に適したフォーマット、例えば、DVB-S(Digital Video Broadcasting-Satellite)に対するコンフォーマント(conformant)である。前記第１受信器1は、異なるフォーマットでデータが送信されるが、前記ホームネットワーク2を介して、前記データの一部または全部を端末装置で使用できるようにする。従って、前記第１受信器1は、配信ネットワークゲートウェイ、すなわち１つまたはそれ以上の配信ネットワークと、１つまたはそれ以上のホームネットワークセグメントに接続される装置である。前記配信ネットワーク（すなわち、前記衛星ネットワーク）がOSI層のいずれかにおいて前記ホームネットワークセグメントに相互接続されるように、それは、１つまたはそれ以上の接続コンポーネントを含んでいる。それは、異なるリンク層技術を相互接続するブリッジまたはルータとして機能できる。すなわち、前記OSI４層以上における機能性も提供するゲートウェイとしての役割を果たせる。結果として、フォーマットという用語は、ネットワークのあるタイプのプロトコルスタックに前記データが一致するよう適合させる方法を意味している。第１ネットワーク（前記衛星ネットワーク）は、前記リンク層レベル、前記ネットワーク層レベルまたは前記トランスポート層レベルのうちの１つまたはそれ以上で異なっていることを意味している前記ホームネットワーク2と異なるプロトコルスタックを有している。ここで留意すべきことは、データがフレーム及び/またはパケットで送信される前記第１受信器1は、前記ホームネットワーク2の前記プロトコルスタックと一致するために、パケットヘッダ及び/またはリセグメント(re-segment)パケットペイロードを追加、除去または変更しなければならない。前記パケットという用語は、通信ネットワーク内のユニットとして送信されるデータの小区間である(refer to)。それは、セルとして知られるパケットのタイプだけでなく、フレームとして一般的に知られる前記ネットワーク層より下のレベルでのパケットを含んでいる。パケットは、ヘッダまたはトレーラ(trailer)と、ペイロードとを具備する。パケットフォーマットは、前記ペイロードの大きさに関するとともに前記ヘッダ/トレーラに含まれる種々のフィールドに関する前記パケットの構成である。

【００３１】

図３は、前記第１受信器1のコンポーネントを概略的に示している。それ（第１受信器1）は、前記MPEGトランスポートストリームを具備するベースバンド信号を取り出すために、搬送波を除去するチューナー/復調器31を備える。前記第１受信器1は、前記パケットを処理するためにプロセッサ32及びメモリ33を用いる。前記プロセッサ32は、システムバス

34に接続されている。この例では、スマートカードリーダ35、モデム36及びイーサネット（登録商標）カード37が前記システムバスに接続される。前記モデム36及びイーサネット（登録商標）カード37は、ネットワークアダプタとして機能する。すなわち、それらは、前記プロセッサ上で動作する適切なソフトウエアと一緒にネットワークのために正しいプロトコルによるネットワークを介してデータが交換されることができるリンクインタフェースを実行する。スマートカード38は、１つまたはそれ以上のプログラムを受信するための権限を提供するために、前記スマートカードリーダ35に挿入される。前記スマートカード38に代わるものとして、他のタイプの携帯用安全装置、例えば、USBドングルまたはPCMCIAフォーマットカードが用いられてもよい。権限を提供するためのソフトウエア実行(software-implemented)安全モジュールも考えられる。この例では、前記ホームネットワーク2は、イーサネット(登録商標）となっている。すなわち前記セットトップボックス3、デジタルテレビジョンセット5及びパーソナルコンピュータ6は、また、イーサネット(登録商標）カードを具備する。しかしながら、ホームネットワークのいずれか他のタイプ、例えば、USB接続、IEEE 1394、IEEE 802.11などを使用することが重視される(stressed)。

【００３２】

本発明によると、前記第１受信器は、前記DVB-Sフォーマット内の前記トランスポートストリームを受信する。次いで、前記PAT及び前記PMT内の複数の前記PIDを用いることによって、それは、どの基本ストリームが前記EMM及び前記ECMのどちらかを備えるか決定するとともに、どれが前記コンテンツデータ、EPGデータ、あるいはIPデータなどを備える基本ストリームであるかを決定する。前記スマートカード38が前記第１受信器1に適切な制御語を取り出すことの権限を与える情報を具備する場合、後者（ECMs）を備える前記トランスポートストリームの一部または全部は、デスクランブルされる。このために、前記スマートカード38は、前記プロセッサ32に前記制御語を戻すために、前記デスクランブリングが実行される複数の前記ECMを処理する。

【００３３】

次いで、前記解読データストリームは、再パケット化される。これは、それら（解読データストリーム）が前記適当な長さのペイロードに分けられ、そして前記ホームネットワーク2で用いられた前記プロトコルで定義された必要なヘッダを付加されることを意味する。次いで、これらのパケットは、再解読される。同じ制御語は、前記ホームネットワーク2のデータパケットフォーマット内の前記パケットを再暗号化するために用いられる。同じキースキームが用いられるので、前記エンタイトルメントメッセージを備える前記トランスポートストリーム内の前記データが、単に転送される。新しいエンタイトルメントメッセージはフォーマットされない。

【００３４】

前記第１受信器1は、前記スマートカード38なしでは前記エンタイトルメントメッセージを解読すること、または前記コンテンツデータをデスクランブルすることはできないという理由で、前記第２受信器と実質的には異ならないことが知られている。それ（前記第１受信器1）は、それ自体のエンタイトルメントメッセージを形成することもできない。これは、前記第１受信器1が相対的に単純であることと、それのCAシステムが認可されていないアクセスに対して前記コンテンツデータを守るための用途で残っていることを前記総括局が保証することの二重の利点を有する。

【００３５】

前記第１受信器1は、前記TSパケット14を前記ホームネットワーク2に対するフォーマットに再パケット化する。この例では、前記ホームネットワークプロトコルスタックは、前記リンク層レベルでイーサネット(登録商標）を、前記ネットワーク層レベルでIPを、そして前記トランスポート層レベルでUDPを用いる。図４は、前記ホームネットワーク2を介して送信されたパケットの構成を示している。いくつかの、例えば、７つのTSパケット14がIPパケット（IPデータグラムの別名でも知られる）39の前記ペイロードを形成する。前記IPパケット39は、UDPヘッダ40及びIPヘッダ41をさらに備える。前記IPヘッダ41は、前記IPパケット39が目的とする前記第２受信器のアドレスを備える。すなわち、それ（前記

IPヘッダ41）は、マルチキャストアドレスを備えてもよい。前記IPパケット39は、プリアンブル43、宛先アドレス44、ソースアドレス45、タイプ46及びCRCチェックサム(checksum)47を備えるイーサネット(登録商標）フレーム42の前記ペイロードを形成する。前記宛先アドレス44は、それらを目的とする前記イーサネット(登録商標）フレームを取り出すために、前記第２受信器によって用いられるブロードキャストアドレス、マルチキャストアドレスまたはユニキャストアドレスである。IP及びUDPヘッダ41,40を付加せずに、前記イーサネット(登録商標）フレーム42内の前記TSパケット14を直ちにカプセル化することも可能であることが知られている。しかしながら、イーサネット(登録商標）を介してIPを用いることは、広範囲に渡って前記データを送信することを可能にする。

【００３６】

好適には、出願人の同時係属国際出願WO 02/07378に全面的にさらに記載されているように、前記第１受信器1は、前記スタックのもとで暗号化の一形態を用いる。

【００３７】

本発明の好適な実施形態では、前記第２受信器は、前記ホームネットワーク2を介して前記第１受信器1に選択コマンドを送信することができる。これらの選択コマンドへの応答において、前記第１受信器1は、いかなる前記第２受信器によっても要求されない前記マルチプログラムトランスポートストリーム内のそれらの基本ストリームを、フィルタをかけて除去する。従って、それ（前記第１受信器）は、各第２受信器に基本データストリームのサブセットのみ送信することができる。

【００３８】

また、前記第２受信器のそれぞれは、スマートカードリーダを備える。挿入されたスマートカードは、それら（前記第２受信器のそれぞれ）が前記第１受信器1から受信されたデータのストリームから複数の前記ECMを取り出すとともに、ある基本ストリームをデスクランブルすることができるようにする。

【００３９】

また、前記第１受信器1は、前記モデム36を用いて前記TSパケットを受信できる。この場合、前記TSパケットは、IPパケット内ですでにカプセル化されていてもよい。しかしながら、複数のイーサネット(登録商標）パケット内でカプセル化される代わりに、前記受信されたIPパケットは一般的に、前記リンク層レベルでPPPパケットまたはATMセルに運び込まれる。それ故に、前記第１受信器1は、イーサネット(登録商標）フレームフォーマット内の受信されたデータを再送信するために、本発明による方法を実行しなければならない。

【００４０】

上記のように、前記第１受信器1は、解読されたデータストリームを再パケット化する。本発明の範囲内で、前記第１受信器1の別の変形が可能である。この変形例では、前記第１受信器1は、第１フォーマット内の符号化された情報を備える第１データストリームを受信し、第２フォーマット内の前記情報を再符号化し、前記第２データストリームの少なくとも１つで前記再符号化された情報を備えるデータを含むように構成される。このいわゆるトランスコーディング(transcoding)は、前記受信されたデータの非圧縮（伸長）及び再圧縮を必要とする可能性がある。一例として、前記第１受信器1は、前記MPEG-4標準により符号化及び圧縮されたプログラム基本ストリームを取り出すためにトランスポートストリームを逆多重化してもよいし、前記符号化されたビデオデータを逆圧縮してもよいし、前記MPEG-2標準によって前記ビデオデータを再圧縮及び符号化してもよい。次いで、トランスコードされた(transcoded)ビデオデータは、パケット化されるとともに前記１つまたはそれ以上の第２受信器に送信されるトランスポートストリーム内にオーディオ及びデータを含んでいる他の関連プログラム基本ストリームによって、多重化される。当然ながら、MPEG-4からMPEG-2へのトランスコーディングは、まさに好都合な例である。データが再送信される場合、前記第１受信器1は、静止画像を、例えば、JPEGからGIFにトランスコードするように構成される。これらの実施形態は、前記第２受信器によってサポートされない異なったフォーマットに放送局が切り換えられた場合、第２受信器としてレガシー

(legacy)受信器を用い続けることが可能であるという有利な効果を有する。次いで、前記第１受信器1内で使うことが必要なだけである。特に、前記再圧縮の別の効果は、前記ホームネットワーク2及び前記配信ネットワークで利用可能な異なった帯域幅を考慮することができる。

【００４１】

好適には、前記第１データストリームの提供者は、情報の第２配信を制御するために別の手段が与えられる。これを実行する１つの方法は、それぞれが認可された受信器が前記キースキームによって暗号化された暗号化データストリームを解読できる複数の異なるエンタイトルメントメッセージを提供することである。各エンタイトルメントメッセージは、少なくとも１つの端末の規格(specification)を備える。言い換えると、前記放送ソース8から前記第１受信器1まで送信された複数の前記ECMのいくつかは、同じ制御語を含んでもよいが、受信器の異なる規格（１つまたはそれ以上の特定装置のタイプまたは識別のどちらか）を含んでもよい。前記第１受信器1は、受信されたデータストリームを復号化するために、それ自体を特定化する複数の前記ECMを取り出す。それは、第２受信器が一致する規格を備えるそれら複数の前記ECMのみを各第２受信器へ送信する。

【００４２】

配信を制御するための別の手段は、少なくとも１つの前記第２端末に少なくとも１つの前記第２データストリームの送信を許可するメッセージを転送することを含んでいる。前記メッセージは、再配信が許可されるかどうかだけを特定する、単一メッセージであってもよい。すなわち、それ（前記メッセージ）は、第２受信器の特定タイプまたは第２受信器の特定最大数への再配信に限られる。前記第１受信器1は、権限が受信されたそれらの第２端末にそれら第２データストリームのみを送信するように構成される。装置特有のECMsと協同して、前記第１受信器1は、例えば、前記データへ同時にアクセスできる第２受信器の数を制限するために、特定の前記ECMsをフィルタして除去することができる。

【００４３】

本発明は、説明してきた実施形態に限られるものではないが、添付の請求項の範囲内において複数の方法で変形させることができる。例えば、前記スクランブルされたデータは、IPパケットを備えてもよい。この場合、前記第１受信器1は、前記データを再送信する前にTSパケット内の前記カプセル化を除去してもよい。

【図面の簡単な説明】

【００４４】

【図１】本発明が用いられるデジタル放送構造の概略図である。

【図２】トランスポートストリームパケットの構成を示す概念図である。

【図３】本発明による端末の構成要素を示す概念図である。

【図４】本発明による端末によって生成されるデータパケットの構成を示す概念図である。

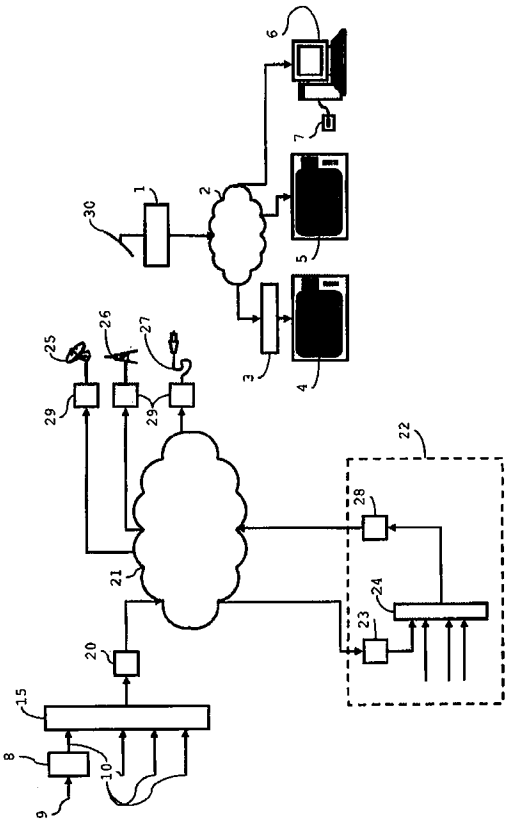
【符号の説明】

【００４５】

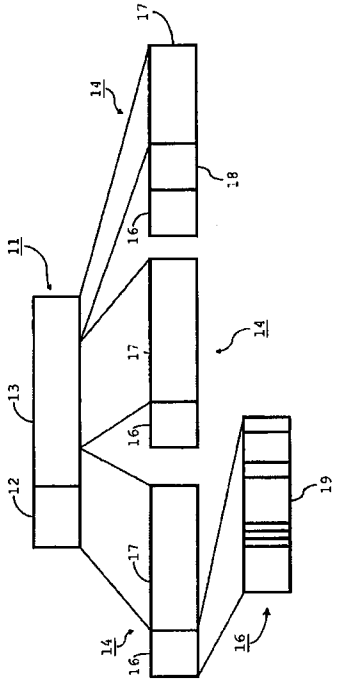
１　第１受信器
２　ホームネットワーク
３　セットトップボックス
４　アナログテレビジョンセット
５　デジタルテレビジョンセット
６　パーソナルコンピュータ
７　スマートカードリーダ
８　放送ソース
９　基本ストリーム
１０　MPEG-2トランスポートストリーム
１１　PESパケット
１２　PESパケットヘッダ

１３　PESパケットペイロード
１４　MPEG-2 TSパケット
１５　MPEG-マルチプレクサ
１６　TSパケットヘッダ
１７　TSパケットペイロード
１８　適応フィールド
１９　パケット識別子
２０、２３、２８、２９　ネットワークアダプタ
２１　第１ネットワーク
２２　総括局
２４　ビットストリーム/マルチプレクサ
２５　衛星送信器
２６　地上送信器
２７　ケーブル送信器
３０　衛星放送受信アンテナ
３１　チューナー/復調器
３２　プロセッサ
３３　メモリ
３４　システムバス
３５　スマートカードリーダ
３６　モデム
３７　イーサネット(登録商標) カード
３８　スマートカード
３９　IPパケット
４１　IPヘッダ
４２　イーサネット(登録商標) フレーム
４３　プリアンブル
４４　宛先アドレス
４５　ソースアドレス
４６　タイプ
４７　CRCチェックサム

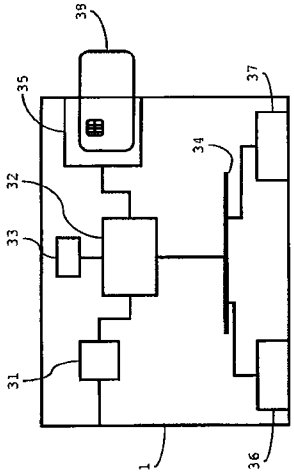
【図１】



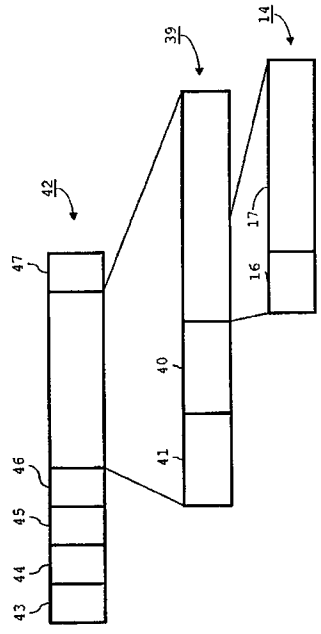
【図２】



【図３】



【図４】



フロントページの続き

(74)代理人 100107836
弁理士 西 和哉
(74)代理人 100108453
弁理士 村山 靖彦
(74)代理人 100110364
弁理士 実広 信哉
(72)発明者 カーシック・ランジャン
アメリカ合衆国・ノースキャロライナ・２８６０１・ヒコリー・サークル・エヌ・イー・ナインティーンス・アヴェニュー・１９９２

Ｆターム(参考) 5C063 AB03 AB05 AC01 AC10 CA23 CA36 DA07 DA13
5C064 BA01 BB05 BC11 BC16 BC20 BD08
5J104 DA04
5K030 GA08 GA15 HA08 HB02 HD01 JA11 JT02 KA19